基于媒体融合的数据中心网络安全加固建设研究

吴红辉
（南京市高淳区广播电视台，江苏 南京 211300）

摘 要：目前我国颁布推行的各项战略决策，有效地促进了互联网的发展，也让互联网思维逐步融入生活生产之中。并且，传统媒体和新媒体逐步融合，逐渐成为我国战略实施的落脚点，在多方影响因素综合作用的结果下，人们的生产生活质量被大大提升。由于网络安全和社会稳定、国家平稳运行紧密相关，并且网络数据中心包含着目标群体的使用数据和机密文件，与此同时还为多方使用者提供数据传输、数据互换的业务。因此，在媒体的大环境下，数据中心网络安全建设显得格外重要，并且亟待解决。只有保障好数据中心网络安全，才可以营造一个国家安全的大环境，切实保护好人民的生产生活。本文基于当前媒体融合下加强数据中心网络安全建设的意义，提出加固网络安全的策略，同时设计网络安全方案的框架，以期能为日后研究提供参考。

关键词：数据中心；安全防护措施；网络安全建设；框架设计；安全设计　**中图分类号：**TP393　**文献标识码：**A
文章编号：1671-0134（2021）03-114-03　**DOI：**10.19483/j.cnki.11-4653/n.2021.03.032
本文著录格式：吴红辉．基于媒体融合的数据中心网络安全加固建设研究 [J]. 中国传媒科技，2021（03）：114-116.

导语

伴随着互联网信息行业的变革，以移动互联网技术，如：自媒体、新媒体短视频等形式的信息时代已经到来。各种信息技术的综合作用，将有边界网络逐渐改变为无边界网络，从前的全台网有限边界逐渐被取代。由于开放性增加，因此在安全形势上面临着十分严峻的挑战，安全问题突出。在媒体融合的背景下，我们必须大力加强网络安全工作的推进，保障网络安质量，保障数据中心的安全，才能更好地在未来的发展中站稳脚步。

1. 数据中心概述

随着信息技术的飞速发展，数据中心的建设已经经历了几十年的历程。在 40 年代时有了数据中心发展雏形——ENIAC，即 Electronic Numerical Integrator And Computer（电子数字积分计算机）的简称，1946 年专为美国弹道研究实验室存储火力表而研制。在当时的环境下，只有该计算机可以满足使用要求，此计算机拥有 17468 个真空管和 7，200 水晶二极管，1，500 中转，70，000 电阻器，10， 000 电容器，1500 继电器，6000 多个开关。[1] 由于设备的组成量庞大，每秒执行 5000 次加法或 400 次乘法，是继电器计算机的 1000 倍、手工计算的 20 万倍。随后在 50 年代，数据中心虚拟化技术商业化，出现了晶体管计算机，即：TRADIC。60 年代时，虚拟化概念逐步进入人们的视野之中。在 80 年代，模块化数据中心出现，它将通常数据中心的设备都部署在集装箱里面，因此又名集装箱数据中心，并且其可以被运往世界任何一个地方。这种数据中心虽然没有传统的数据中心的恢弘气势，但它的建设成本极低，大约是传统数据中心建设成本的 1%，并且由于体积小赋予了灵活的机动性，部署周期较短。到现代，转变为云数据中心。

数据中心是支持公司的业务操作和未来的发展的核心。主要包括以下方面：“综合服务器、应用平台，集中到一体的备份和储存模式；统一的平台管理系统，以客户为中心的运营管理组织和流媒体”。这逐渐使得数据中心的业务从单一业务模式发展到多种业务，规模逐步扩大。信息技术在企业中发挥着越来越重要的作用，数据中心正在从单纯的消费模式转型为投资和收入模式。[2]

2. 媒体融合下加强数据中心网络安全建设的意义

2.1　数据中心网络安全是信息化时代治国理政的牢固基石

现如今人们在工作之余，谈论和使用一些自媒体和新媒体已经习以为常，上至六七十岁的老人，下至五六岁的孩童，在网络媒体的运用上都十分熟练。但是目前我国网络信息平台上信息冗杂，并且还存在各种风险与隐患，因此安全问题显得十分重要。总之，维护数据中心、网络安全就是在保护我国的政治和文化安全。

由于大众传播量高和人际传播广的特征，互联网在构建和谐社会方面具有重要作用。随着 IT 行业的高速发展，我国政策解读的方式也逐渐从原来的传统媒体转向新兴媒体。应用更多的新型技术，将最新出台的政策、方针、战略等广泛的推广开来。相比于传统模式，此种方式成本更低，效率更高，人民更易接受。并且政府可以利用互联网技术将管理模式、管理体系进行创新，扩大电子渠道在日常办公、业务中的作用。在疫情环境下，人民可以通过网络平台对工作进行监督，政府也可以通过网络平台向人民传达国家政策，对政策进行解读，使人民可以及时接收到信息。政府工作人员通过网络平台与人民进行沟通，既保障了安全也保证了工作效率。[3]

2.2　数据中心网络安全是我国成为网络强国的重要基础

随着互联网信息技术的不断发展，信息化和网络安全是我国国家安全和国家发展的重要战略问题。这和我国广大人民的生活、工作是息息相关的。我们必须从整体把握大局，在多方协调下将我国逐步建设为网络强国。其中最基础又最重要的环节就是要将基础设施建设完全，

并且完善各项还在发展中的技术，使其具备强势的抵御入侵的能力。我们要将媒体融合下的数据中心网络安全置于实现网络强国战略目标的首要位置，在未来的竞争中，我们要牢固地占领上层建筑中政治、文化等领域的优势地位，通过使用网络技术来使国家更加强大。

3. 媒体融合背景下维护数据中心网络安全的途径

3.1 严格遵守数据中心网络安全建设原则

针对数据进行的多种操作，如访问、使用、破坏、修改等措施，足以证明数据是数据中心网络安全维护的重中之重。我们不从硬件设施切入，而是从网络数据中心来看，网络是数据中心安全运行的基本平台，起着数据的传输作用。所以在对数据中心网络安全建设时，务必要遵守以下原则：

首先，在建设时应该合理的划分网络的安全区域，并且不同区域之间权限要层次分明，这样可以保证客户在使用时通过身份认证提供准确无误的许可授权，防止非法人员的入侵以及恶性的资料盗窃和损坏事件的发生。[4]

其次应该建设一个可靠性高的网络平台。在此平台上通过提高安全等级，保证数据的安全准确的传输。防止数据在传输过程中被篡改和读取，并且提供对网络支撑平台本身的安全保护，保证网络平台能够平稳高效地运行。综上所述，我们在数据中心网络安全建设时，务必从整体上把握大局，不可以将安全问题完全寄托在一种手段，或者预防方法上；并且要采用多种措施，将系统的安全防护措施进行多样化，采用多重保障来保证其安全；并且在建设时要本着操作简便、管理容易的原则，采用最新的安全技术以实现管理程序的自动化并且减轻管理的负担。

3.2 将舆论导向牢牢掌握

将传统媒体与新兴媒体进行融合发展，促使媒体行业整体的格局发生了一定程度的变化。舆论斗争的主战场从原来的传统媒体转向互联网，这是我们国家、我们党中央从宣传国家软文化、提升国家文化软实力所做出的政策上的决定。为了将舆论导向牢牢地掌握在自己手中，我们必须以先进的技术作为支撑。在媒体融合的大背景下，要想通过舆论导向将主动权掌握在自己手中，我们必须在技术上占据一定的优势，从而才能在激烈的市场竞争中处于优势地位。为了达到此种目的，我们必须将基础设施尽快完善。虽然目前我国在互联网信息技术中的个别领域处于一定的优势地位，但基础设施相比于其他许多发达国家仍处于落后阶段。我们必须尽早打破核心技术和设备受制于人的局面，这对于我们想要将舆论导向掌握在自己手中是十分不利的。所以，在目前媒体融合的过程中，我们必须大力完善各种基础设施，多方协调才能更好地掌握舆论自主权。

与此同时我们将针对超出掌控的舆论现象，做好网络舆情反应机制。现在网络十分发达，用户可以随时将所见所闻上传到网络平台上，几小时之后便可以伴随着用户的转发量的不断增高和各方看法的不断汇集，最终发酵并且达到高潮。如果不能很好地掌控这种局面，而是对发生的情况进行回避，不进行正面的疏导，这无疑会增加负面影响，不利于我们掌握舆论。只有健全网络舆情监测系统和完善反应机制，定期对网络上的舆论进行积极的汇报和引导，针对敏感问题进行正面的回复和解决，回应社会、人民所关切的问题，才有利于我们维护网络安全，将舆论主导权掌握在自己手中。

3.3 在网络安全管理体系中勇于创新

要通过有效的、科学性高的方式进行媒体管理。推动媒体在党的正确领导下与数据中心网络平台飞速融合发展，对于网络上和现实中不同的行业形态意识进行高效、科学、合理的管理。[5]

我们应该转变管理的理念。在做任何行动前，只有思想达到了一定深度，管理体系的创新才可以达到一定高度。在传统媒体与新媒体融合的背景下，以往的传统管理模式不再是大众所能接受的，并且对于媒体融合背景下，该种管理方式也不见得可以 100% 奏效。管理方式必然应该同媒体融合趋势共同进步，二者相辅相成，才可以达到更高的高度。在互联网信息时代，我们必须更加注重网络上的行为产生的影响，让用户对其所作所为负责，对自己的网络言行把关，同时也对他人进行监督。各大平台群的群主、板块的版主、小站的 up 主等责任人有义务对“内部”人员进行管理。

并且我们应该将首席信息安全官制度大力推广。该体系是维护网络信息安全的重要体系，首席安全官起到了为本机构定制信息安全战略、预测可能发生的风险事件、向高层领导进行汇报并且提出解决问题的可行办法。目前该种方式在国外的某些国家已经得到广泛应用，我国应该将其引入，取其精华去其糟粕，结合我国现有环境形式，使得该种模式成为我们自己的体系，细化维护网络安全的过程，从而更好地针对数据中心网络安全加固建设做出贡献。

4. 网络安全方案框架设计

4.1 设计思路

该设计针对融媒体平台未来的发展，对公司的安全保障服务、计算能力以及资源服务等方面提出要求，通过引进成熟先进的技术，来调整并改进数据中心建设整体框架，基于融媒体中心的建设，将云计算作为核心，从而实现以服务为核心的建设方式。

该设计方案需要采用如下图所示安全框架，需要做好边界安全、整网安全可视以及数据安全等等。边界安全包括很多方面，分别是安全域隔离能力、网络优化能力以及用户管理能力。安全域隔离能力主要是指能够对网络区域进行分割，从而限制各个区域之间的流量，精细控制网络流量，避免出现大规模的安全风险[6]。网络优化能力要求能够对用户应用的网络提供灵活的流量管

理能力，从而保障关键用户与应用的网络带宽，保障数据传输的质量。用户管理能力，主要是对管理接入网络的用户行为，包括控制网络访问行为、限制访问资源以及身份认证等等。

伴随互联网的发展，其已经逐渐成为人们生活中必不可少的一个依靠，然而信息安全问题也逐渐严峻。我国提出需要加强全天候全方位感知网络安全态势，不断强化网络安全的管理。全网安全感知平台通常由两方面构成，分别是安全感知系统和威胁潜伏探针，具有较高的服务响应能力，还能够进行深度分析，这在一定程度上提高了网络数据的安全处理性能。安全感知系统基于大数据能够进行流量监测、数据分析等，从而实现海量数据分析的全方位检测。



图 1

4.2　融媒体中心安全设计方案

4.2.1　边界安全

做好边界安全防护，首先需要了解哪些网络边界需要防护，这往往要通过安全分区设计来确定。在本次设计方案中有很多边界，分别是安全管理边界、内网办公边界、融媒体平台边界、公有云 / 专属云边界、省级平台边界以及网络总体出口边界。

4.2.2　数据中心云安全

本设计基于虚拟化架构的等保一体机安全平台，来建立云平台租户 / 租户边界的南北向安全防护体系。等保一体机架构基于软件虚拟化，借助信息安全技术、服务链管理以及 Overlay 技术等技术来实现一种自适应安全技术架构。并且由于等保一体机拥有开放性的特点，能够支持第三方安全组建集成，可以给用户提供功能完善的云安全服务市场。

4.2.3　主机安全

服务端点安全主要由控制中心和虚拟端点 agent 构成。端点 agent 需要能够安装在全部的主机上，要包含全部的物理主机、云主机以及虚拟机等等。管理平台要部署在本地。在完成基本的数据采集之后，端点 agent 会把有用的数据信息发送到控制中心，然后通过管理平台进行全局的汇总和安全的分析。

4.2.4　全网态势感知

第一，资产业务管理。根据功能来划分，内网设备可以分为两个方面，分别是资产与业务。资产配置详情展示板块，能够对传输使用协议、开放端口、操作系统以及内网服务器资产的 IP 地址等进行识别。业务与资产关系展示模块，可以按照资产 IP 地址 / 地址段，共同构成特定的业务组。

第二，监测识别知识库。监测识别知识库能够对大量的数据信息进行识别，具备将强的识别能力。

第三，可视化平台。全网攻击检测可视化平台支持安全态势感知，能够对全网安全事件以及攻击的地图展现与可视化展现。可视化平台能够支持全网业务可视化，能够呈现全网业务对象的访问关系以及被入侵业务的图形化展示。还支持用户自定义的业务资产管理的可视化。

第四，风险可视化。根据等保部分要求，能够对高危用户的违规业务、违规行为、攻击行为以及风险操作进行可视化展示。

第五，大数据分析引擎。大数据分析引擎主要负责实现大数据关联分析能力以及各类检测能力。这一引擎主要由数据预处理、模型融合、模型构建、数据融合以及分析结果生成等模块组成，能够极大程度上地提升数据中心网络安全的能力。

结语

在媒体融合背景下维护数据中心网络安全是信息化时代下做出的战略选择，也是互联网信息技术发展的必然趋势。我们伟大中国的复兴正在路上，要攻克的艰难险阻还不止于此，在该问题上我们必须充分意识到目前存在的问题并且给予足够的重视，立足于我国基本国情，坚持发展与安全齐头并进，在全体人民和工作者的共同努力下建设网络强国。媒

参考文献

[1] 蔡高伟 . 基于媒体融合的数据中心网络安全加固建设研究 [J]. 广播电视网络，2020，364（04）：74-76.

[2] 王云波 . 关于媒体融合背景下网络安全的思考 [J]. 传媒论坛，2019，45（21）：94-94.

[3] 赵 芃 . 媒体融合背景下的网络安全问题研究 [J]. 科技传播，2016，8（1）：198-200.

[4] 徐俭 . 全媒体新闻融合生产与发布平台设计考虑要点 [J]. 电视工程，2015（003）：49-53.

[5] 王菲 . 媒介大融合：数字新媒体时代下的媒介融合论 [M]. 广州：南方日报出版社，2007.

[6] 孙源 . 融媒体建设环境下的信息安全如何保障 [J]. 西部广播电视，2018，439（23）：46-47.

作者简介：吴红辉（1971-），男，江苏南京人，工程师，研究方向：广播电视技术。

（责任编辑：胡杨）